kyndryl

Kyndryl Managed Extended Detection and Response

Customer Presentation

Contents

01 Why Kyndryl?

02 How does Kyndryl view the situation?

03 How can we help?

kyndryl

What sets Kyndryl Security & Resiliency apart:

- Extensive partner ecosystem to support best-in-class technology solutions
- Improved ability to identify and respond to security threats
- More efficient security teams with flexible, modular delivery models

Leader

NelsonHall Cyber Resiliency NEAT Leader for 2024 [1]
Cybersecurity Services 2022 RadarView Report by Avasant [2]

50+

countries with Kyndryl Security and Resiliency presence

7500+

Skilled Security and Resiliency practitioners globally

6

Global Security Operations Centers

500+

Security and Resilience patents

40+

Security and Resiliency alliances and strategic partners

30+ years

Experience in IT services

NelsonHall NEAT Leader 2024 Report [1]
Avasant Cybersecurity Services 2022 RadarView [2]

kyndryl

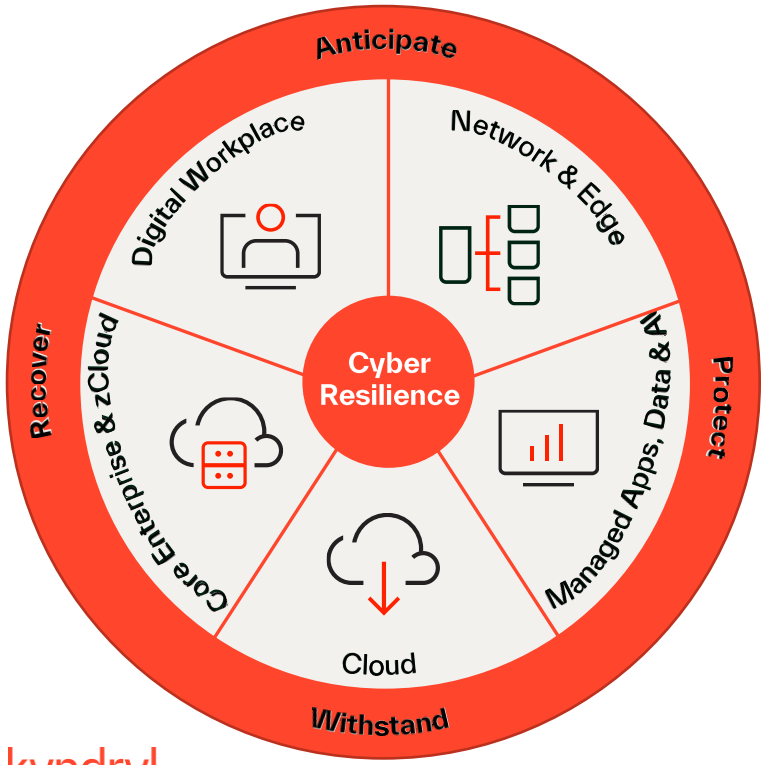
Kyndryl's Cyber Resilience Framework

cyber resilience

[**sahy**-ber ri-**zil**-y*uh*ns, -**zil**-ee-*uh*ns]

noun

The ability to anticipate, protect against, withstand and recover from adverse conditions, stresses, attacks and compromises of cyber-enabled business.



Security Assurance Services

Assess and benchmark resilience maturity, gain visibility into significant threats and vulnerabilities, manage compliance

- Risk Management
- Offensive Security Testing
- Compliance Management

Zero Trust Services

Protect critical business data and applications in a security-rich infrastructure

- Identity & Access Management
- Endpoint Security
- Network Security
- Data Protection & Privacy

Security Operations & Response Services

Discover and respond to a detected security incident

- Incident Response and Forensics
- Threat Detection & Response
- Vulnerability Management
- Security Operations Center (SOC) Services
- Security Operations as a platform

Incident Recovery Services

Mitigate impact of disruption with capabilities to automatically recover critical business processes and data

- Cyber Incident Recovery
- Managed Backup Services
- Hybrid Platform Recovery
- Data Center Design & Facilities

Anticipate → Protect → Withstand → Recover

Cybersecurity + Recovery

Deep expertise | Proven Processes | Intelligent automation

kyndryl

Defending against cybercrimes has never been harder

Growing frequency, speed, and targeting of threats

Microsoft security researchers have tracked a **200% increase** in ransomware attacks.[1]

Security gaps from fragmented tools

80 security tools for an average sized organization.[2]

Alert fatigue and SOC burnout

2 in 5 security leaders feel they are at risk due to cybersecurity staff shortage.[2]

The security team's work is endless

How do I investigate more effectively?

How do I prioritize?

How do I prevent and stop attacks quickly?

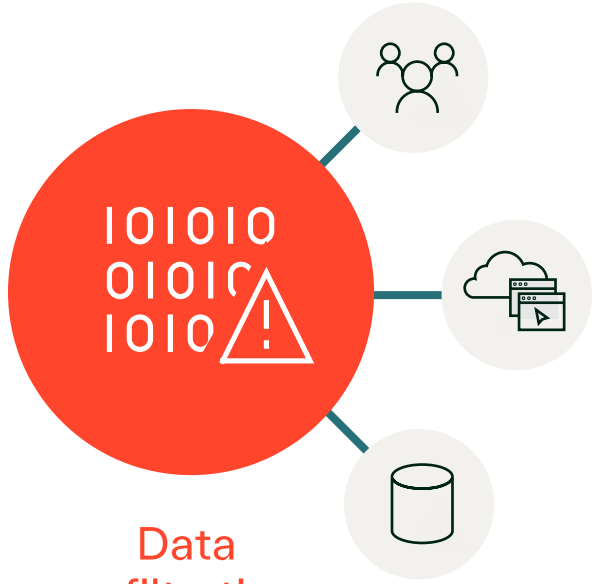
1. Microsoft Digital Defense Report 2023 (MDDR) | Microsoft Security Insider
2. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

kyndryl

Sophisticated attacks cross multiple domains

Human-operated ransomware campaign

Business email compromise campaign



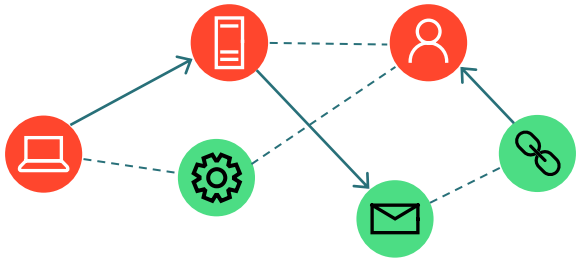
Data exfiltration

Email | Endpoints | Identities | SaaS Apps | Data | Cloud Workloads

XDR is the answer to modern attacks

EDR

VS.



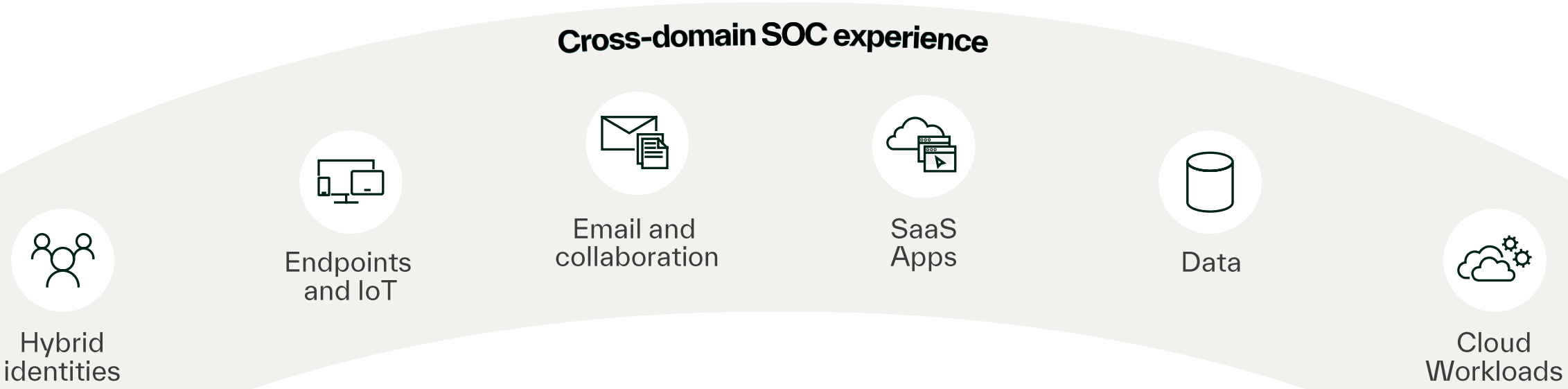
XDR

EDR	XDR
Endpoint security only	Holistic security and signal correlation across identity, email, endpoint, SaaS app, data, cloud, and more
Siloed endpoint alerts	Incident-based investigation and response experience
Can only help fend off endpoint-specific attacks and lacks the big picture to help with advanced attacks	Protects against advanced attacks such as ransomware, business email compromise (BEC), and adversary in the middle (AiTM)

kyndryl

Kyndryl Managed Extended Detection and Response

Build a unified defense with XDR



Prevent

Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management

Protect

Automatically contain and remediate compromised assets

Detect and Respond

Use incidents to respond to cross-workload threats from a single portal

Speed up response with an experience designed for SOC efficiency

Extend

Unified APIs and connectors

kyndryl

Kyndryl's Approach to Managed Extended Detection and Response

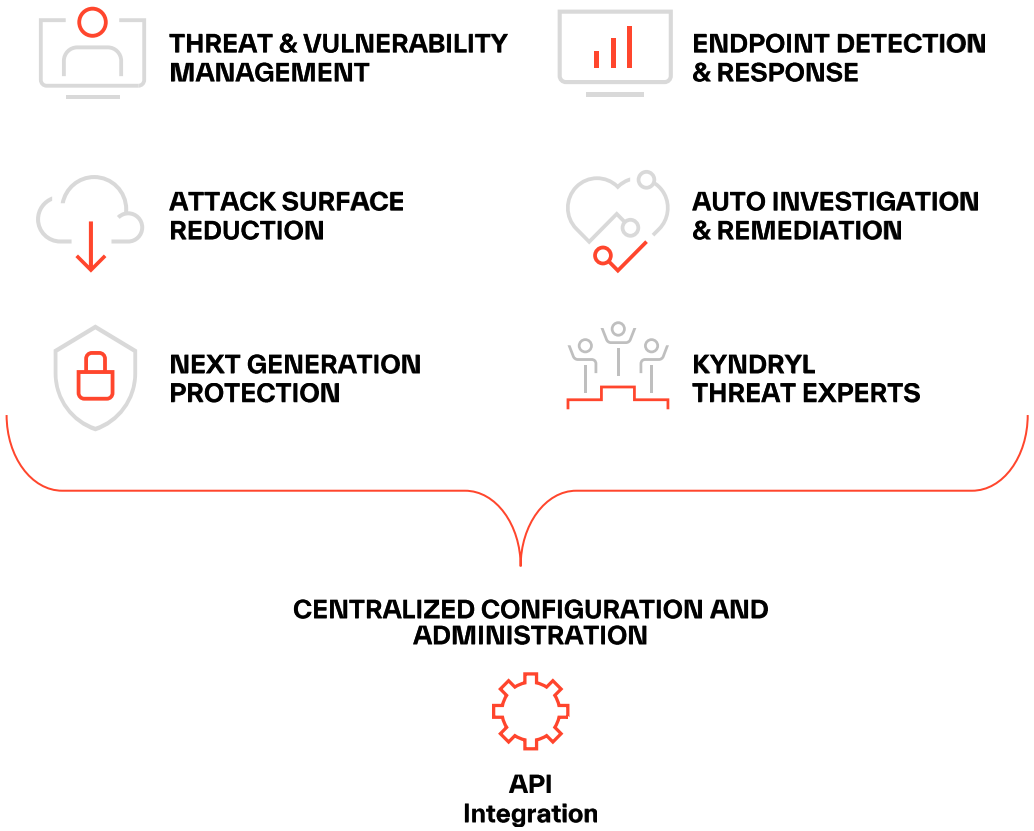
Customer Challenges

- XDR deployment requires internal buy-in from stakeholders that may be resistant to change.
- Limited automation is the biggest constraint.
- Collecting and correlating detections across various security layers.
- Integrating XDR with existing security investments can be complex.

Kyndryl's Managed Extended Detection and Response Benefits

- Complete XDR design, planning, migration, and managed services.
- Timely delivery and a well-defined process.
- Kyndryl's XDR methodology and risk-based delivery model with a Zero Trust lens.
- 24x7 incident, alert, investigation, and response services.
- Continuous XDR secure configuration, user, policy, and privilege management.
- Architecture design for migration that includes detection rules, playbooks, historical data, dashboarding, and other processes.
- Architecture planning and support.
- Support from Microsoft's technology modernization program.

Extended Detection and Response



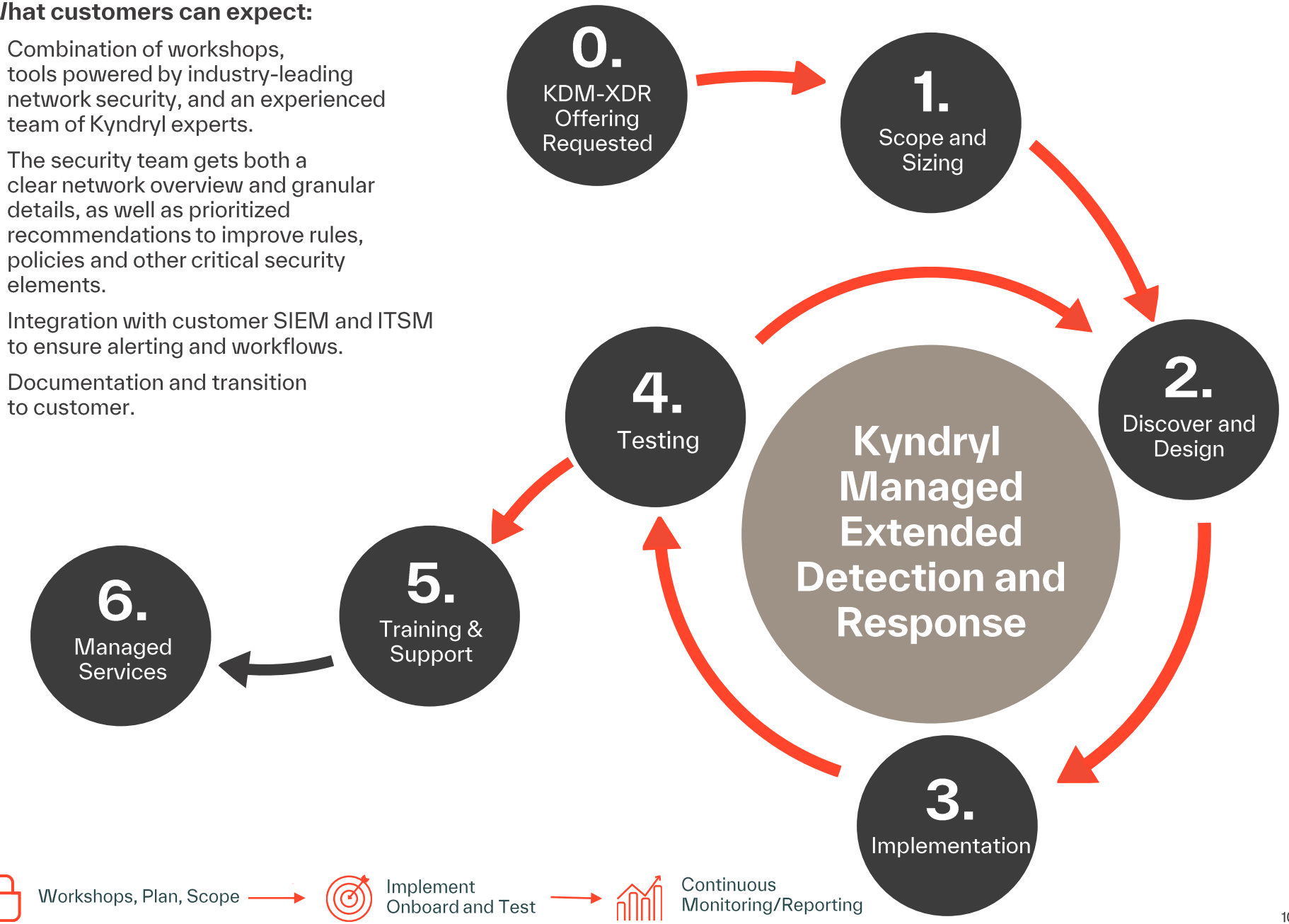
Kyndryl Managed Extended Detection and Response Delivery Approach

Diagram shows the Kyndryl Delivery Methodology for Kyndryl Managed XDR

- Kyndryl's XDR Implementation covers steps 0–4
- Step 5: Can be added on by Kyndryl Consult Services
- Step 6: Can be added on with XDR Managed Services

What customers can expect:

- Combination of workshops, tools powered by industry-leading network security, and an experienced team of Kyndryl experts.
- The security team gets both a clear network overview and granular details, as well as prioritized recommendations to improve rules, policies and other critical security elements.
- Integration with customer SIEM and ITSM to ensure alerting and workflows.
- Documentation and transition to customer.



kyndryl

Kyndryl Extended Detection and Response Implementation Services

Overview

Kyndryl will provide Extended Detection and Response (XDR) Implementation Services intended to leverage the timeliness and urgency of today's ransomware attacks to motivate organizations to see the visibility of their endpoint security in their production environment. Kyndryl XDR Implementation Services consists of the design, deployment and operational handover of the XDR processes, reporting and technology, applying the principles of the Zero Trust framework.

XDR Deployment Services

- Environmental assessment
- Definition of Customer's threat profile, goals, devices baseline, onboarding priority and definition of implementation timeline
- Response plan and security policies definitions and agreement (example is to define what response actions are allowed to be performed and under what conditions)
- Architecture planning and support
- Guidance on how to deploy endpoint software and/or automated deployment of software endpoint
- Onboarding of Customer's approved users
- Endpoint baselining and policy tuning (e.g., white labeling of wrongly terminated applications)

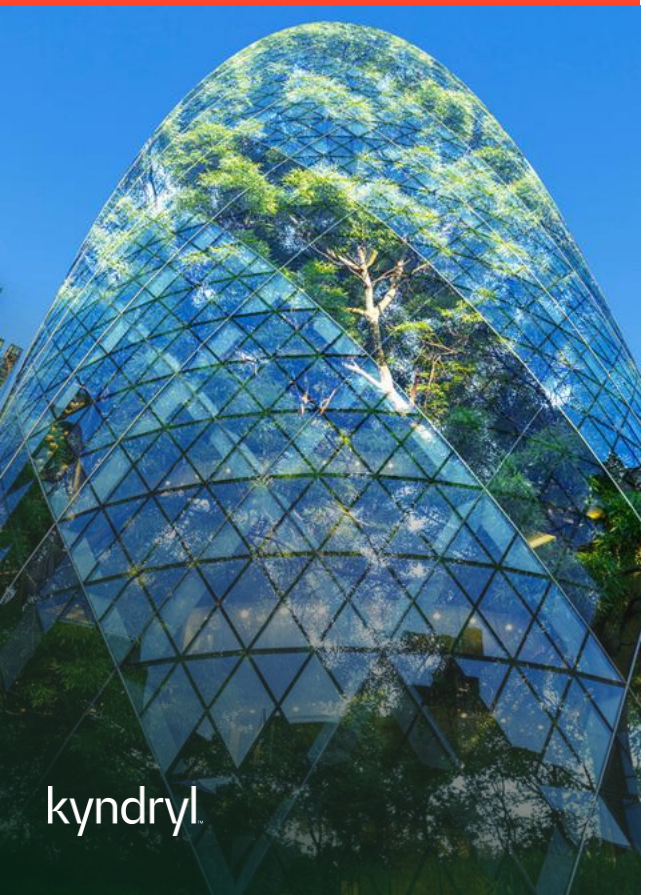
Service Modules

- Service planning
- Policy and response plan definition
- Initial 30 days baselining and tuning

Supported Vendor Products

- Microsoft Defender

Kyndryl Managed Extended Detection and Response



Kyndryl Managed Extended Detection and Response (XDR) is designed to protect a Customer's endpoints by combining the power of the most modern and recognized XDR solutions with an 24x7 elite team of senior security professionals ready to identify, investigate and stop the most sophisticated and advanced cyberattacks.

The Managed XDR Services protect the Customer's endpoints detecting malware, including ransomware variants, zero-days, non-malware, and file-less attacks by leveraging the tool of choice and by configuring and managing it in accordance with industry best practices and the Customer's business needs.

Key Offering Capabilities

- Standard framework to onboard and manage endpoints agent and XDR console
- Policy design, continuous review and tuning in accordance with best practices and Customer needs
- Console and agent health and status management
- 24x7 incident, alert, investigation and response services
- Threat hunting via additional detection capabilities and techniques to identify adversary activity

Available Service Modules

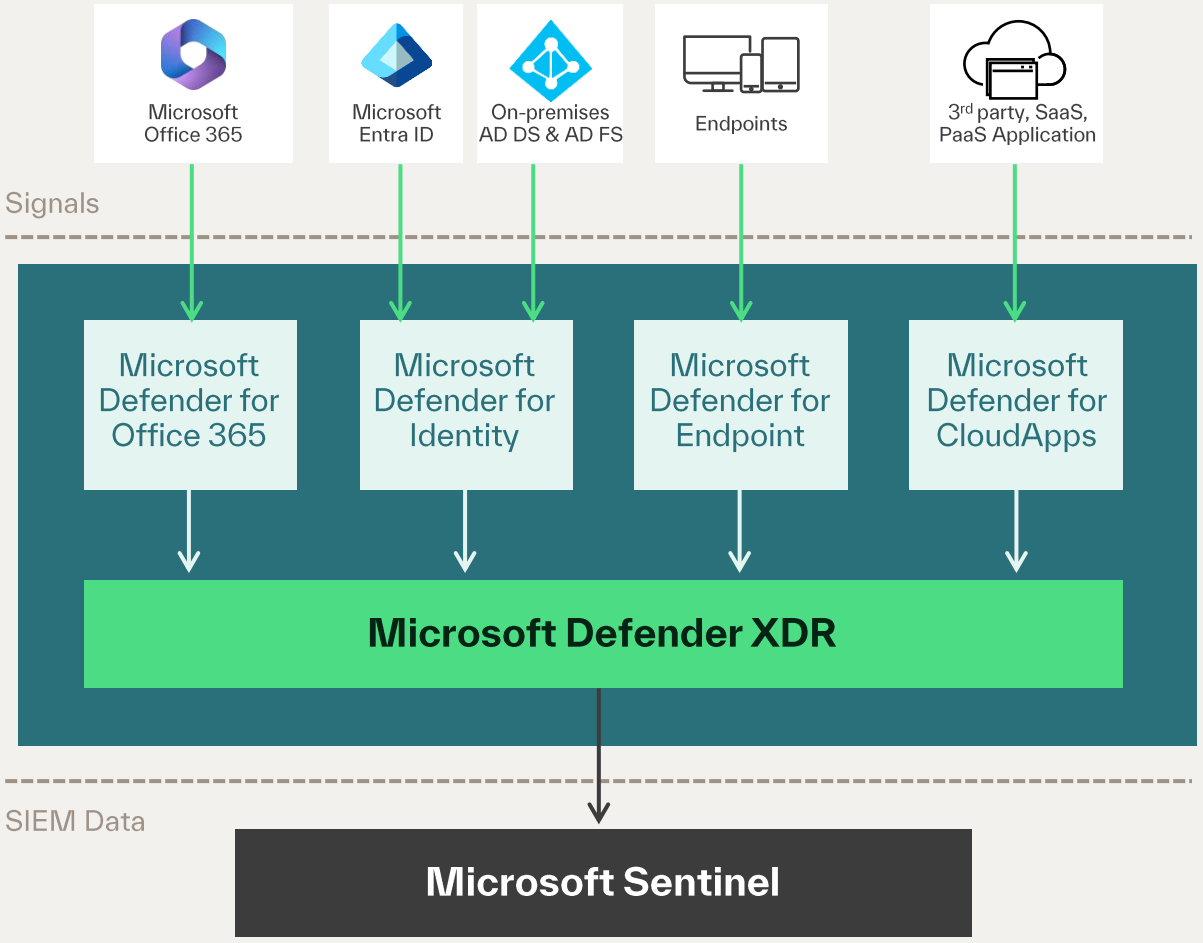
- XDR Deployment Services
- 24x7 M-EDR (Managed Endpoint Detection and Response Services)
- XDR Threat Hunting Services

Supported Vendor Products

- Microsoft Defender

Architecture Overview

- Technologies in Scope
  - Microsoft Defender for Extended Detection and Response (baseline)
    - Microsoft Defender XDR
    - Microsoft Defender for Endpoint
    - Microsoft Defender for Office 365
    - Microsoft Defender for Identity
    - Microsoft Defender for Cloud Apps
  - Migrate existing XDR solution to Microsoft Defender for XDR
  - Kyndryl's internal tools for monitoring
- Delivery model: remote
- On-site requirements will be custom
- Alerting, monitoring, and ticketing flows from platform
- Supported vendor: Microsoft Defender
- System must communicate with all managed XDR components for management
- Alerting/ticketing forwarded to customer ITSM, email, or SMS
- Complete reporting
- Kyndryl Bridge Console Dashboard integration with Microsoft XDR



kyndryl

How Kyndryl Experts for XDR Managed Services Works

Triage

Filter the noise to prioritize Microsoft Defender XDR incidents and alerts that matter and alleviate alert fatigue

Investigate

Investigate and analyze the most critical incidents first and document progress and findings

Respond

Contain and mitigate incidents faster by delivering step-by-step guided and managed response, and consult on-demand via chat

Prevent

Provide detailed recommendations and best practices to go beyond detection and response to prevent future attacks

Continuous security posture improvements

Kyndryl Managed Extended Detection and Response

Addresses common pain points and gaps

- Lack of or difficult to maintain the level of skilled personnel
- Reduces high management costs caused by the increasing number of agents, security alerts and false positives
- Simplifies management of an increasingly complex architecture encompassing more and more remote endpoints using a mix of operating systems and deployment models as Cloud

Our differentiators

- Security integration with other competencies: Delivery team working as a single organism by informing and collaborating globally across service lines
- Actively partnering with new technology providers to bring the best products to market
- Ability to support our customers' existing endpoint security infrastructure

We succeed when our customers succeed

kyndryl

Thank you

Notices and Disclosures

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only.
Actual performance results may vary depending on specific configurations and operating conditions.